What is claimed is:

1. A method of improving security policy administration and enforcement using a role-permission model, comprising steps of:

identifying one or more groups of permitted actions on selected resources;

assigning a name to each identified group;

defining each assigned name to a security system as a security object; and

associating subjects with each assigned name.

2. The method according to Claim 1, wherein the assigned name is a role name.

3. The method according to Claim 1, wherein the selected resources are executable methods.

4. The method according to Claim 1, wherein the selected resources are columns of a database table.

5. The method according to Claim 1, wherein the selected resources are rows of a database table.

6. The method according to Claim 1, wherein the selected resources are files and the permitted actions are file access operations.

7. The method according to Claim 1, wherein the selected resources are function calls to

functions of one or more executable programs.

8. The method according to Claim 1, wherein the selected resources are Enterprise JavaBeans ("EJBs") and the permitted actions are methods on the EJBs.

9. The method according to Claim 1, wherein the selected resources are servlets and the permitted actions are methods of the servlets.

10. The method according to Claim 1, wherein the selected resources are Uniform Resource Identifiers ("URIs") and the permitted actions are methods which reference the URIs.

11. The method according to Claim 1, wherein the selected resources are JavaServer Pages ("JSPs") and the permitted actions are methods referenced from the JSPs.

12. The method according to Claim 1, wherein the selected resources are any resource that is expressible to the security system and the permitted actions are selected from a set of actions that are permitted on those resources.

13. The method according to Claim 1, further comprising the steps of:

receiving an access request for a particular one of the selected resources;

determining one or more roles which are required for accessing the particular resource;

determining an identity of a source of the access request;

for each of the required roles, until obtaining a successful result or exhausting the required roles, determining whether the identity of the source is associated with the required role; and

authorizing access to the particular resource only if the successful result was obtained.

14. The method according to Claim 13, wherein the step of determining the one or more roles further comprises consulting a collection created from the identified permitted actions on the particular resource.

15. A system for improving security policy administration and enforcement in a computing network using a role-permission model, comprising:

means for identifying one or more groups of permitted actions on selected resources;

means for assigning a name to each identified group;

means for defining each assigned name to a security system as a security object; and

means for associating subjects with each assigned name.

16. The system according to Claim 15, further comprising:

means for receiving an access request for a particular one of the selected resources;

means for determining one or more roles which are required for accessing the particular resource;

means for determining an identity of a source of the access request;

for each of the required roles, until obtaining a successful result or exhausting the required roles, means for determining whether the identity of the source is associated with the required role; and

means for authorizing access to the particular resource only if the successful result was obtained.

17. A computer program product for improving security policy administration and enforcement in a computing network using a role-permission model, the computer program product embodied on one or more computer readable media and comprising:

computer readable program code means for identifying one or more groups of permitted actions on selected resources;

computer readable program code means for assigning a name to each identified group;

computer readable program code means for defining each assigned name to a security system as a security object; and

computer readable program code means for associating subjects with each assigned name.

18. The computer program product according to Claim 17, further comprising:

computer readable program code means for receiving an access request for a particular one of the selected resources;

computer readable program code means for determining one or more roles which are required for accessing the particular resource;

computer readable program code means for determining an identity of a source of the access request;

for each of the required roles, until obtaining a successful result or exhausting the required roles, computer readable program code means for determining whether the identity of the source is associated with the required role; and

computer readable program code means for authorizing access to the particular resource only if the successful result was obtained.